ACADEMIA | Letters

Lessons from the GDPR in the COVID-19 era

Omer Rana
Jose Llanos
Madeline Carr

As the coronavirus (COVID-19) pandemic keeps claiming human lives and ravaging the global economy, governments, businesses and individuals have turned to digital technologies to both contain the virus and adapt to the 'new normal'. To interrupt the chain of transmission more effectively, numerous contact-tracing apps - which notify people that they have been in close proximity with COVID-19 carriers - have been rolled out globally. Restaurants, pubs and hospitality businesses have embraced a multitude of mobile apps allowing customers to book tables, place orders and make payments remotely and without human contact, in a move to protect their staff and facilitate social distancing. In response to lockdown measures, people have flocked to the Internet to work, conduct business, stay close with friends and relatives, find entertainment and more. In fact, Facebook, Amazon and YouTube have reportedly lowered the quality of video streaming in Europe to reduce the strain on Internet networks,[1] and companies like Netflix and Zoom have experienced dramatic growth.[2]

In this context of expanding datafication of our health and every other aspect of our lives, the COVID-19 pandemic has stress tested not only our healthcare infrastructure but also the soundness of Europe's General Data Protection Regulation (GDPR) following its entry into force about two years ago. Two important trends can be discerned from this test. First, ob-

[1] Mark Beech, 'COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal' (*Forbes)*https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/.

[2] Dominic Rushe and Benjamin Lee, 'Netflix Doubles Expected Tally of New Subscribers amid Covid-19 Lockdown' (*the Guardian*, 21 April 2020) http://www.theguardian.com/media/2020/apr/21/netflix-new-subscribers-covid-19-lockdown; Iman Ghosh, 'Zoom Is Now Worth More Than the World's 7 Biggest Airlines' (*Visual Capitalist*, 15 May 2020) https://www.visualcapitalist.com/zoom-boom-biggest-airlines/.

Corresponding Author: Omer Rana, omerrana.cardiff@gmail.com
Citation: Rana, O., Llanos, J., Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. *Academia Letters*, Article 429. https://doi.org/10.20935/AL429.

servance of the GDPR has overall impeded the deployment of excessively invasive contact-tracing-based surveillance to contain the virus. Second, as we increase reliance on digital technologies during the pandemic, it becomes virtually impossible to prevent more aspects of our lives from being intensively monitored by both established big tech firms and a growing number of private actors. These two trends combined reveal a transparency and accountability gap between the public and the private sector which warrant innovative solutions to uphold our fundamental rights to privacy and protection of personal data.

The GDPR has kept contract-tracing-based surveillance in check

In countries with low data protection standards, contact-tracing apps typically gather highly sensitive data, including location data and biometrics.[3] This data is then sent to a centralised server, oftentimes located in government offices. This data can be subsequently paired with existing public and corporate datasets, thus revealing intimate details of people's lives, even providing grounds for discrimination. In addition to ignoring privacy-by-design standards, most of these apps are closed source, which means they do not allow for third-party review or security audits.[4] Access to individuals' data by government agencies, as well as aggregation of diverse datasets and data-sharing between governments and private companies, commonly takes place with little to no oversight or transparency.

Conversely, in the early days of the pandemic the European Commission and the European Data Protection Board issued guidelines on the GDPR-compliant development of COVID-19 apps and associated initiatives.[5] These bodies largely promoted individuals' control over personal data (by requiring that the adoption of COVID-19 apps be voluntary),[6] sought to avoid the undue identification and tracking of individuals (based on requirements that only minimal, necessary and/or anonymised data be processed),[7] and generally ensured that any emergency restrictions on individual freedoms be proportionate and limited to the emergency period.[8]

[3] See examples of contact-tracing apps in Bahrain, China, Ecuador, India, Russia, Singapore, Turkey and more countries in Freedom House, 'Freedom on the NET 2020: The Pandemic's Digital Shadow' (2020) 15 *et seq*.

[4] *ibid 15.*

[5] European Commission, 'Commission Recommendation on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data'; European Commission, 'Guidance on Apps Supporting the Fight against COVID-19 Pandemic in Relation to Data Protection C(2020) 2523 Final'; EDPB, 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak'.

[6] European Commission (n 5) 3; EDPB (n 5) 7.

[7] European Commission (n 5) 8–9; EDPB (n 5) 4–7.

[8] European Commission (n 5) 6; EDPB (n 5) 8.

Corresponding Author: Omer Rana, omerrana.cardiff@gmail.com
Citation: Rana, O., Llanos, J., Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. *Academia Letters*, Article 429. https://doi.org/10.20935/AL429.

The majority of EU Member States' Data Protection Authorities (DPAs) have been actively involved in the development and implementation of COVID-19 apps and other data-driven measures to tackle the crisis, issuing recommendations and discussing bills introducing derogations from data protection safeguards.[9]

Following the aforementioned guidelines and recommendations, most EU countries have launched government-backed COVID-19 apps built on privacy-preserving architectures which use a Bluetooth low energy connection to automatically detect and trace all COVID-19 contacts of handheld device users, estimating their proximity on the basis of signal intensity.[10] Bluetooth proximity data has a privacy advantage over GPS-based data because the only information it involves is anonymised contact tokens, which can be cryptographically secured in a way that is less vulnerable to de-anonymisation than location history.[11] The great majority of government-supported contact-tracing apps implemented in the EU do not collect GPS-based data.[12] Instead, they process only Bluetooth proximity data, typically based on the decentralised Google-Apple Exposure Notification API.[13] In this way, the potential for mission creep during and after the pandemic are ameliorated, and an adequate balance between EU residents' data privacy and the public interest is struck.

The GDPR remains inadequate to curb private sector surveillance

The pandemic has multiplied the scenarios where our consent to multiple forms of opaque and unwarranted data processing and sharing is forcefully extracted, thereby compounding the risks that our digital identity - largely constructed without our involvement or approval - be relied upon to make decisions contrary to our interests.

For example, imagine you want to have a meal in your local pub (when restrictions are relaxed). Upon entering the premises, you realise there is no 'traditional' customer service; rather, you need to download a booking and payment app, entering personal details to register. However, registration cannot be completed - and therefore you cannot be served - until you

[9] See generally European Union Agency for Fundamental Rights, 'Coronavirus Pandemic in the EU - Fundamental Rights Implications: With a Focus on Contact-Tracing Apps / Bulletin 2' (2020) 46–51.

[10] Matteo Ciucci and Gouardères Frédéric, 'Policy Department for Economic, Scientific and Quality of Life Policies - European Parliament - National COVID-19 Contact Tracing Apps' (2020) PE 652.711 1.

[11] Vi Hart and others, 'Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 Wile Mitigating Privacy Risks' (Edmond J Safra Center for Ethics 2020) 17 https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf?m=1586179217.

[12] See updated list in Sheet 'Contact Tracing Apps: Overview' at https://docs.google.com/spreadsheets/d/1enCBRLVCo2Dp2B0AB3tEYvLc279i5LUuoGCzoelz8aQ/editgid=2010667918

[13] For an overview of this protocol see ICO, 'Opinion: Apple and Google Joint Initiative on COVID-19 Contact Tracing Technology' (2020) Reference 2020/01.

Corresponding Author: Omer Rana, omerrana.cardiff@gmail.com
Citation: Rana, O., Llanos, J., Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. *Academia Letters*, Article 429. https://doi.org/10.20935/AL429.

tick a box signalling acceptance to terms and conditions that allow for extensive collection of personal data for multiple purposes unrelated to the transaction you had in mind (*i.e.* having a simple meal). This type of consent is clearly invalid under the GDPR. Yet, without the competent DPA actually finding and penalising the breach, consent obtained in this way is 'fair game'. Data hoovered from your frequent visits to the pub can lead to predictions of a medical condition based on inferred alcohol consumption, ultimately resulting in a more expensive health insurance premium.

Moreover, as we are forced to conduct most of our activities online, the likes of Facebook, Google and Amazon have more of our attention - and therefore more of our personal data. As a result, they get even better at permanently assessing, categorising and ultimately nudging us into acting in a given way, such as clicking on an ad, registering for a service, purchasing a product, viewing specific content, and even voting for a certain political candidate. Consequently, we are turned into Pavlovian dogs of the digital age, unaware of both the manipulation that takes place online and the underlying privacy invasions that enable it.

In spite of the GDPR's stringent consent standards and expanded transparency requirements, we remain unable to make informed choices about data processing and exercise meaningful control over our personal data.

Halting private sector surveillance warrants innovative solutions

The adequacy of the EU data protection framework to resist digital surveillance by states and its inadequacy to prevent the same practice by private actors is explained by a transparency and accountability deficit in the private sector. Overall, EU Member States' institutionality and democratic processes involve suitable 'checks and balances' against disproportionate state surveillance initiatives. Although non-binding, governments normally follow the guidance from EU-level data protection watchdogs and DPAs. A government may be tempted to depart from these regulators' recommendations and implement instead more intrusive measures.[14] In these cases, however, scrutiny by and mounting pressure from diverse stakeholders normally result in their withdrawal.[15]

[14]Such as the Norwegian government's contact-tracing app 'Smittestopp', which continuously tracked and uploaded people's GPS location onto a national database for half a year. Amnesty International, 'Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy' (16 June 2020 https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/.

[15]For example, after criticism by activists, technologies and scholars, the Norwegian DPA imposed a temporary ban on 'Smittestopp', ultimately resulting in its permanent demise. Kristin Sandvik, 'Big Data & Society: The Norwegian Covid-19 Tracing App Experiment Revisited' (*Big Data & Society*, 3 November 2020)

Corresponding Author: Omer Rana, omerrana.cardiff@gmail.com
Citation: Rana, O., Llanos, J., Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. *Academia Letters*, Article 429. https://doi.org/10.20935/AL429.

Conversely, the advent of the digital economy has seen the consolidation of a surveillance infrastructure featuring a vast universe of private actors, the majority of which seeks to process our personal data for financial gain, irrespective of our privacy preferences. Since the processing of personal data takes place in a 'black box', we cannot verify which types of our personal data is processed, for what purposes, or with whom it is shared – let alone prevent specific forms of data processing which are increasingly likely to harm us. In addition, being notoriously under-resourced and understaffed, DPAs[16] are increasingly unable to effectively enforce compliance with data protection law by an overwhelming and growing number of actors.[17] Lack of transparency in data flows coupled with poor law enforcement means that unlawful private sector surveillance is regularly unpunished. Apart from the very rare occasions when a DPA steps in, controllers have no real incentive to change their lucrative practices other than the very remote threat of a fine.

Ultimately, just as there is no single effective response against COVID-19, there is no silver bullet solution to protect our data privacy. Having a robust data protection regulation like the GDPR is an essential safeguard; however, law on paper becomes meaningless if it is systematically violated in ways regulators cannot realistically and effectively monitor, detect and punish. The GDPR must be accompanied by measures capable of correcting the transparency and accountability deficit in the private sector, and governments' response to the COVID-19 pandemic might have just hinted a potential approach to this end.

Just as partnerships between public and private actors have been formed to leverage state-of-the-art mobile technology to determine whether we have been in close proximity to COVID-19 carriers, similar partnerships can leverage blockchain technology to create a reliable audit trail of personal data flows and enforce compliance with GDPR rules through 'smart contracts'.

A blockchain is an append-only database (or *ledger*)composed of sets (*blocks*) of cryptographically signed transactions that is shared, synchronised and stored in a decentralised fashion, based on a consensus algorithm.[18] Blockchains provide confidence that stored information (for example, an account balance, property certificates or data flows) cannot and

http://bigdatasoc.blogspot.com/2020/11/the-norwegian-covid-19-tracing-app.html; Similarly, after strong criticism by privacy advocates, the UK abandoned the NHSX app and developed another one based on Google-Apple Exposure Notification API. Natasha Singer, 'Virus-Tracing Apps Are Rife With Problems. Governments Are Rushing to Fix Them.' *The New York Times* (8 July 2020 https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html.

[16]Johnny Ryan and Alan Toner, 'Europe's Governments Are Failing the GDPR - Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities' (2020).

[17]Access Now, 'Two Years under the EU GDPR - An Implementation Progress Report' (2020) 7.

[18]See generally Daniel Drescher, *Blockchain Basics* (Springer 2017).

Corresponding Author: Omer Rana, omerrana.cardiff@gmail.com
Citation: Rana, O., Llanos, J., Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. *Academia Letters*, Article 429. https://doi.org/10.20935/AL429.

has not been tampered with, thus ensuring a 'single truth' across different participants which contribute to maintaining the ledger.

A privacy-preserving blockchain-based stack is being developed in the Privacy-aware Cloud Ecosystems (PACE) project.[19] This privacy-enhancing technology (PET) maps out and stores all data flows arising from a person's interaction with a cloud-based service, denying access to certain kinds of data based on the user's preferences, and reporting violations to regulators. Given their potential of increasing much needed transparency in data flows and affording users control over their personal data at scale, this and other similar PETs are steps in the right direction to replicate the effect the GDPR has when states attempt disproportionate intrusions into our data privacy.

[19] EPSRC: EP/R033439/1

Corresponding Author: Omer Rana, omerrana.cardiff@gmail.com
Citation: Rana, O., Llanos, J., Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. *Academia Letters*, Article 429. https://doi.org/10.20935/AL429.